Examples
MDS codes

16^{th} February, 2006

1. Consider the matrix

$$A = \begin{bmatrix} 3 & 5 & 6 & 2 & 1 \\ 4 & 4 & 6 & 1 & 3 \\ 2 & 5 & 2 & 1 & 6 \end{bmatrix}$$

over $GF(7)$. Show whether minimum distance separable (MDS) codes can be obtained from A. If they could, find two such codes and give either a generator matrix or a parity check matrix for each of them. Then give the code words and encoding functions for each.

Solution. Examine the values of determinant of all submatrices of A. We have, $\begin{vmatrix} 3 & 5 \\ 4 & 4 \end{vmatrix} = 6$,
$\begin{vmatrix} 3 & 6 \\ 4 & 6 \end{vmatrix} = 1$, $\begin{vmatrix} 3 & 2 \\ 4 & 1 \end{vmatrix} = 2$, $\begin{vmatrix} 3 & 1 \\ 4 & 3 \end{vmatrix} = 5$, $\begin{vmatrix} 5 & 6 \\ 4 & 6 \end{vmatrix} = 6$, $\begin{vmatrix} 5 & 2 \\ 4 & 1 \end{vmatrix} = 4$, $\begin{vmatrix} 5 & 1 \\ 4 & 3 \end{vmatrix} = 4$, $\begin{vmatrix} 6 & 2 \\ 6 & 1 \end{vmatrix} = 1$, $\begin{vmatrix} 6 & 1 \\ 6 & 3 \end{vmatrix} = 5$,
$\begin{vmatrix} 2 & 1 \\ 1 & 3 \end{vmatrix} = 5$, $\begin{vmatrix} 3 & 5 \\ 2 & 5 \end{vmatrix} = 5$, $\begin{vmatrix} 3 & 6 \\ 2 & 2 \end{vmatrix} = 1$, $\begin{vmatrix} 3 & 2 \\ 2 & 1 \end{vmatrix} = 6$, $\begin{vmatrix} 3 & 1 \\ 2 & 6 \end{vmatrix} = 2$, $\begin{vmatrix} 5 & 6 \\ 5 & 2 \end{vmatrix} = 1$, $\begin{vmatrix} 5 & 2 \\ 5 & 1 \end{vmatrix} = 2$, $\begin{vmatrix} 5 & 1 \\ 5 & 6 \end{vmatrix} = 4$,
$\begin{vmatrix} 6 & 2 \\ 2 & 1 \end{vmatrix} = 2$, $\begin{vmatrix} 6 & 1 \\ 2 & 6 \end{vmatrix} = 6$, $\begin{vmatrix} 2 & 1 \\ 1 & 6 \end{vmatrix} = 4$, $\begin{vmatrix} 4 & 4 \\ 2 & 5 \end{vmatrix} = 5$, $\begin{vmatrix} 4 & 6 \\ 2 & 2 \end{vmatrix} = 3$, $\begin{vmatrix} 4 & 1 \\ 2 & 1 \end{vmatrix} = 2$, $\begin{vmatrix} 4 & 3 \\ 2 & 6 \end{vmatrix} = 4$, $\begin{vmatrix} 4 & 6 \\ 5 & 2 \end{vmatrix} = 6$,
$\begin{vmatrix} 4 & 1 \\ 5 & 1 \end{vmatrix} = 6$, $\begin{vmatrix} 4 & 3 \\ 5 & 6 \end{vmatrix} = 2$, $\begin{vmatrix} 6 & 1 \\ 2 & 1 \end{vmatrix} = 4$, $\begin{vmatrix} 6 & 3 \\ 2 & 6 \end{vmatrix} = 2$, $\begin{vmatrix} 1 & 3 \\ 1 & 6 \end{vmatrix} = 3$, $\begin{vmatrix} 3 & 5 & 6 \\ 4 & 4 & 6 \\ 2 & 5 & 2 \end{vmatrix} = 5$, $\begin{vmatrix} 3 & 5 & 2 \\ 4 & 4 & 1 \\ 2 & 5 & 1 \end{vmatrix} = 4$,
$\begin{vmatrix} 3 & 5 & 1 \\ 4 & 4 & 3 \\ 2 & 5 & 6 \end{vmatrix} = 5$, $\begin{vmatrix} 3 & 6 & 2 \\ 4 & 6 & 1 \\ 2 & 2 & 1 \end{vmatrix} = 6$, $\begin{vmatrix} 3 & 6 & 1 \\ 4 & 6 & 3 \\ 2 & 2 & 6 \end{vmatrix} = 6$, $\begin{vmatrix} 3 & 2 & 1 \\ 4 & 1 & 3 \\ 2 & 1 & 6 \end{vmatrix} = 3$, $\begin{vmatrix} 5 & 6 & 2 \\ 4 & 6 & 1 \\ 5 & 2 & 1 \end{vmatrix} = 3$, $\begin{vmatrix} 5 & 6 & 1 \\ 4 & 6 & 3 \\ 5 & 2 & 6 \end{vmatrix} = 4$,
$\begin{vmatrix} 5 & 2 & 1 \\ 4 & 1 & 3 \\ 5 & 1 & 6 \end{vmatrix} = 3$, $\begin{vmatrix} 6 & 2 & 1 \\ 6 & 1 & 3 \\ 2 & 1 & 6 \end{vmatrix} = 4$.

Every square submatrix of A is non-singular. From A we may obtain two MDS codes. These are namely the $[8, 3, -]$ code over $GF(7)$ with the generator matrix $G = (\, I_3 \quad A \,)$ and the $[8, 5, -]$ code over $GF(7)$ with the parity check matrix $H = (\, A \quad I_3 \,)$.

#

For the $[8, 3, -]$ code, the generating function is

$$G = \begin{pmatrix} 1 & 0 & 0 & 3 & 5 & 6 & 2 & 1 \\ 0 & 1 & 0 & 4 & 4 & 6 & 1 & 3 \\ 0 & 0 & 1 & 2 & 5 & 2 & 1 & 6 \end{pmatrix}$$

#

Then,

$$(\, a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \quad a_7 \quad a_8 \,) = (\, a_1 \quad a_2 \quad a_3 \,) \begin{pmatrix} 1 & 0 & 0 & 3 & 5 & 6 & 2 & 1 \\ 0 & 1 & 0 & 4 & 4 & 6 & 1 & 3 \\ 0 & 0 & 1 & 2 & 5 & 2 & 1 & 6 \end{pmatrix}$$

and the encoding functions become

$$\begin{aligned} a_4 &= 3a_1 + 4a_2 + 2a_3 \\ a_5 &= 5a_1 + 4a_2 + 5a_3 \\ a_6 &= 6a_1 + 6a_2 + 2a_3 \\ a_7 &= 2a_1 + a_2 + a_3 \\ a_8 &= a_1 + 3a_2 + 6a_1 \end{aligned}$$

#

The code words are

$$C = \{10035621, 01044613, 00125216, 11002534, 10153130, 01162122\}$$

#

For the $[8, 5, -]$ code, from the parity check matrix we know that the generating function is

$$G = (\, I_5 \quad -A^T \,) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 4 & 3 & 5 \\ 0 & 1 & 0 & 0 & 0 & 2 & 3 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 5 \\ 0 & 0 & 0 & 1 & 0 & 5 & 6 & 6 \\ 0 & 0 & 0 & 0 & 1 & 6 & 4 & 1 \end{pmatrix}$$

Then,

$$(\, a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \quad a_6 \quad a_7 \quad a_8 \,) = (\, a_1 \quad a_2 \quad a_3 \quad a_4 \quad a_5 \,) \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 4 & 3 & 5 \\ 0 & 1 & 0 & 0 & 0 & 2 & 3 & 2 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 5 \\ 0 & 0 & 0 & 1 & 0 & 5 & 6 & 6 \\ 0 & 0 & 0 & 0 & 1 & 6 & 4 & 1 \end{pmatrix}$$

and the encoding functions become

$$\begin{aligned} a_6 &= 4a_1 + 2a_2 + a_3 + 5a_4 + 6a_5 \\ a_7 &= 3a_1 + 3a_2 + a_3 + 6a_4 + 4a_5 \\ a_8 &= 5a_1 + 2a_2 + 5a_3 + 6a_4 + a_5 \end{aligned}$$

#

The code is then

$$C = \left\{ \begin{array}{lllll} 43510000, & 23201000, & 11500100, & 56600010, & 64100001, \\ 66011000, & 54310100, & 22410010, & 30610001, & 34001100, \\ 02101010, & 10301001, & 60400110, & 05600101, & 43000011 \end{array} \right\}$$

#